Electrical Power and Energy Systems 62 (2014) 59–65

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

A vulnerability model for power system dynamic security assessment

Jianlan Li *, Shuhong Huang

Huazhong University of Science &Technology, Wuhan 430074, China

ARTICLE INFO

Article history:
Received 2 June 2012
Received in revised form 31 December 2013
Accepted 20 March 2014
Available online 8 May 2014

Keywords:
Power system
Security assessment
Vulnerability
GM(1,1)
Grey correlation moment

ABSTRACT

Traditional security assessment based on risk takes into account the failure probability and the failure consequence. This paper provides a modification on the risk calculation by replacing the failure probability with the current status to overcome the dependence on mass statistical data. The vulnerability model is proposed that incorporates the two key factors of the risk along with the deterioration trend factor to define the system security level, which efficiently indicates the current and potential danger. Grey system theory is used to predict the equipment deterioration trend and the grey correlation moment is defined to evaluate equipment state with multi-parameters. The classification and quantification of equipment state, failure consequence, risk, deterioration trend and vulnerability are discussed. A feed water pump case demonstrates the effectiveness of vulnerability in system dynamic security assessment.

Introduction

Risk is often used as an indicator to assess the security level and provide technical support for condition based maintenance (CBM) decision-making [1–3]. Many maintenance strategy based on risk have been proposed to ensure equipments reliability in oil refinery, petrochemical industry, power plant, etc. [4–7]. Javadian introduces three indexes such as average failure rate, average outage time and average annual outage time for the system's risk analysis of protection system's operation in a test distribution network according to various locations and capacities of Using Distributed Generation [8]. To get realistic severity and risk estimations of contingencies, Krishnan proposes contingency assessment method that takes into account the nature of probability distribution of power system operating conditions [9]. Risk assessments based on Technology Readiness Level (TRL) have been employed in risk models. The objective of Raja is to create a model that is able to draw a correlation between a modified TRL and downtime of a gas turbine engine, thus provided a means of quantitatively measuring the risk [10]. Dusko develops an age-dependent unavailability model for calculating risk related to standby safety. The time-averaged function of the selected risk measure is obtained from probabilistic safety assessment, and further extended with inclusion of additional parameters relate to test and maintenance activities as well as ageing parameters relate to component ageing [11]. Zhou proposes an aging failure model and individual models for common cause outages, following a thorough discussion of modeling and methodology with a real-life example about the power system planning of a Canadian city [12]. George proposes that risk assessment consists of the identification and assessment of hazards and exposures, and applies a procedure for risk assessment to evaluate plant potential economic losses due to risk exposure by the determination of two risk indices, probable maximum loss and maximum foreseeable loss [13]. A joint model of the system operation process based on semi-Markov is proposed and the system multi-state reliability is applied to the reliability and risk assessment of the port oil pipeline transportation [14]. Moreover, fuzzy theory, Total Transfer Capability (TTC), analytic hierarchy process and support vector machine are used in risk for security assessment [15–20].

As we all know, the unit will face more danger when the equipment is in a continuous deterioration status. However, the traditional risk mainly concerns with the failure probability and the failure consequence, while ignoring the impact of performance deterioration trend on system security. Thus, Fouad proposes a concept of system vulnerability as a new framework for power system dynamic security assessment. The new concept combines information on the level of security and its trend. The level of safety is the deviation of system parameters from their threshold values, and the trend index is the sensitivity to the changing system parameter [21]. Chen presents a new approach to calculate the voltage vulnerability for power systems voltage security assessment based on voltage risk index and its trend to load level with changing system conditions [22].

However, the deviations of system parameters from their threshold values are still insufficient to evaluate system current safety level in Fouad's risk model. In fact, the failure consequence

* Corresponding author. Tel.: +86 27 87542817; fax: +86 27 87548658.
E-mail address: hust_ljl@hust.edu.cn (J. Li).

http://dx.doi.org/10.1016/j.ijepes.2014.03.026
0142-0615/

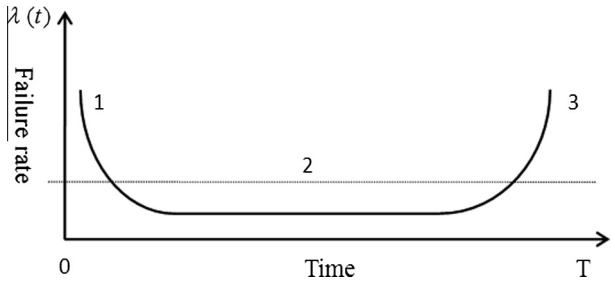

Fig. 1. The bathtub curve of failure rate.

is also an important factor for system safety. It is obviously that the failure with a serious consequence will result in larger danger on system than that with light consequence does. Therefore, both of the current state and the failure consequence shall be considered in current safety level. Moreover, mass statistics data must be used to calculate the failure probability in the traditional risk models. In order to overcome the above mentioned problems in traditional security assessment, this paper proposes a new indicator of vulnerability for system dynamic security assessment. The vulnerability includes the information of equipment current state, failure consequence and its deterioration trend to define the system security level, furthermore, it replace the failure probability with equipment state to avoid the dependence on mass statistical data to make it easy for system security assessment.

This paper is organized as follows: 'section Vulnerability' defines a new risk indicator and a new vulnerability indicator. Deterioration prediction and state assessment are proposed in 'section Deterioration prediction' and 'section State Assessment' respectively. 'Section Vulnerability Quantification' presents the vulnerability quantification, and 'section Security assessment of feed water pump' realizes the security assessment of feed water pump by the vulnerability model. Finally, 'section Conclusion' makes the conclusions.

Vulnerability

Traditional risk mainly takes into account two factors, such as the failure probability and the failure consequence. It is often defined as follows:

$$\lambda = p \times s \tag{1}$$

where λ is the equipment risk indicator, p is the equipment failure probability, and s is the equipment failure consequence. According to Eq. (1), equipment with high failure probability or serious failure consequence will result in severely dangerous on system.

Based on the reliability analysis, the equipment state is always in the cycle of normal-fault-repair-normal during its whole lifetime. The change of equipment state is a stochastic process and often meets certain probabilistic statistical distribution. The typical failure rate curve is bathtub curve shown in Fig. 1. Curve 1 in Fig. 1 is an early failure period and the failure rate is a decline curve. Curve 2 is a constant failure rate stage in which the failure rate is approximately constant. Equipment failure occurs in this period due to accidental factors such as overload and mishandling. For the reason of ageing, fatigue, and creep, the failure rate increases significantly in curve 3 named exhaust period. Generally, the failure probability curve is obtained according to mass statistical data, yet it is often a difficult task, especially for engineers in power plants due to lack of statistical data. Moreover, the failure probability represents a statistical law in league, and it cannot indicate the real security level of the specific equipment in different operational environments. So, for a specific equipment under specific circumstances, it is difficult to realize the accurate security assessment by Eq. (1).

However, we can find a correlation between failure probability and equipment state. When equipment state is good, its failure probability must be low, that is, its position locates in curve 2 in Fig. 1. If the equipment's characteristic parameters are abnormal, then the equipment failure probability increases and corresponds to curve 3 in Fig. 1. Obviously, it is easier to evaluate equipment state than calculate failure probability. State assessment is based on equipment's characteristic parameters, yet failure probability is the statistical result depending on mass statistical data. Moreover, the equipment state indicates the true health status of specific equipment, which is different with the failure probability based on statistical data. Therefore, it is a feasible way to replace the failure probability with equipment state in risk definition.

In order to overcome the problems of traditional risk definition in Eq. (1), a new risk is redefined:

$$\lambda = c \times s \tag{2}$$

where c is the equipment current state, it is a dimensionless value of equipment state, $0 < c < 1$. The bigger c means the worse status. Obviously, the risk defined in Eq. (2) is calculated by the equipment state rather than the failure probability, therefore, it provides a easy method for security assessment.

Since the risk only take into account equipment current state (or failure probability) and failure consequence, it is a relatively static indicator. However, equipment will inevitably be subject to the interference of various factors during operation, such as fatigue, and wear. The interference will lead the development of equipment towards the trend of deterioration and pose potential threat to system. Therefore, only the equipment current state and failure consequence are still insufficient for system security assessment. This paper argues the equipment deterioration trend should be taken into account as an important factor to perfectly indicate the system security level.

Based on the prediction technology, a predictive deterioration coefficient is defined as follow:

$$\gamma = I(F(x_1, x_2, \cdots x_n)) \tag{3}$$

where γ is the predictive deterioration coefficient, $x_1, x_2, \cdots x_n$ are equipment's characteristic parameters, $F(x_1, x_2, \cdots x_n)$ is the predictive function of deterioration, and $I(F)$ is the deterioration assessment function. The equipment will face higher risk if the equipment begins to deterioration. The predictive result can provide more important information for decision-maker to accurately evaluate system security level.

According to the analysis above, three factors, such as equipment current state, failure consequence and deterioration trend shall be taken into account in the system security assessment. Thus, the vulnerability can be defined as follows:

$$v = \mathrm{c} \times \mathrm{s} \times \gamma = \lambda \times \gamma \tag{4}$$

where v is the vulnerability, it is a dimensionless value, $0 < v < 1$. The bigger v means the lower security level.

It can be seen from Eq. (4) that the vulnerability indicates not only the risk under current operational condition, but also the potential danger in future. Therefore, the vulnerability is a better indicator than the risk defined in Eq. (1) to define the system security level. Moreover, the calculation of vulnerability need not depend on mass statistical data, thus, the vulnerability has better operability than the risk.